Cours du Prof. Anand Dessai — ALGÈBRE ET GÉOMÉTRIE I

SÉRIE 9

À rendre avant le jeudi 21 novembre, 16h

Pour tous les exercices de toutes les séries une justification de votre réponse est attendue !

Soit $f \in \mathbb{Z}[x]$ un polynôme. Le *contenu* de f est le plus grand diviseur commun de ses coefficients. Le polynôme f est dit *primitif* si son contenu est 1 (ou -1).

Exercice 1 (4 points)

1. Soient $f, g \in \mathbb{Z}[x]$ deux polynômes primitifs. Montrez que f divise g dans $\mathbb{Q}[x]$ si et seulement si f divise g dans $\mathbb{Z}[x]$.
2. Déduisez le résultat suivant: Un polynôme primitif $f \in \mathbb{Z}[x]$ est irréductible si et seulement s'il est irréductible dans $\mathbb{Q}[x]$.

Exercice 2 (4 points)

1. Soient $f(x) \in \mathbb{Q}[x]$ et $g(x) = f(x+1) \in \mathbb{Q}[x]$. Montrez que $f(x)$ est irréductible dans $\mathbb{Q}[x]$ si et seulement si $g(x)$ est irréductible dans $\mathbb{Q}[x]$.
2. Soit $p \in \mathbb{N}$ un nombre premier. Montrez que $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ est irréductible dans $\mathbb{Q}[x]$.
3. Montrez que $\mathbb{Z}[x]$ est un anneau factoriel qui n'est pas principal.
4. Montrez que $\mathbb{Q}[x, y]$ est un anneau factoriel qui n'est pas principal.

Exercice 3 (4 points) Quels polynômes sont irréductibles ?

$$
\begin{array}{cc}
x^3 - 1 \in \mathbb{Z}[x] & 7x^4 - 100x^3 - 1000x^2 + 10000x + 10 \in \mathbb{Q}[x] \\
x^7 + 1 \in \mathbb{Q}[x] & x^2y + xy^2 - x - y + 1 \in \mathbb{Q}[x, y] \\
x^3 + x + 1 \in \mathbb{F}_2[x] & x^3 + x + 1 \in \mathbb{F}_3[x] \\
x^3 - 3 \in \mathbb{Q}[x] & x^7 - 2x + 2 \in \mathbb{R}[x]
\end{array}
$$

Exercice 4 (4 points) Soit $p \in \mathbb{N}$ un nombre premier tel que $p \equiv 1 \mod 4$.

(a) Montrez qu'il existe $x \in \mathbb{Z}$ tel que $x^2 \equiv -1 \mod p$.
(*Indication: considérez* $x = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot \frac{p-1}{2}$.)

(b) Montrez que $\mathbb{Z}[i]/(p) \cong \mathbb{F}_p[t]/(t^2 + 1)$.

(c) Utilisez (a) et (b) pour montrer que p n'est pas irréductible dans $\mathbb{Z}[i]$.

(d) Déduisez que p s'écrit comme une somme de deux carrés.
(*Indication: utilisez l'application* $\deg : \mathbb{Z}[i] - \{0\} \to \mathbb{N}$ *vue dans la série 7.*)